CORTAVO™

4 STEPS TO PRIORITIZING TECHNOLOGY GAPS TO BRIDGE FIRST

A technology audit can help you better understand and identify gaps in your company's security, compliance and backup postures. Small and medium-sized businesses (SMBs) can benefit significantly from a technology audit when determining the best way to refresh IT components.

It's much easier to prioritize and address issues that may be affecting your goals and overall vision once you've identified the gaps in your infrastructure through an audit report.

Before you refresh your technology infrastructure, there are four important considerations to make:

1 UNDERSTAND YOUR NETWORK'S MAP AND DEPENDENCIES

- [ ] Before you can begin a technology refresh, you must first map the entire IT infrastructure, including dependencies, failover opportunities and peak usage times. If systems must be taken offline to refresh, they must be done systematically at low-use times so that work is not entirely halted – especially for global teams that work around the clock.

- [ ] It is always advisable to deploy an automated solution that can simplify the process of mapping your IT environment and understanding various dependencies (relationship mapping).

  A properly executed relationship map covers all assets and then creates logical, two-way relationships between them. After that, you can see the dependencies and relationships for a single IT component, making it simple to understand what's vulnerable whenever a problem gets reported within the network. A logical structure enables better information management, which in turn drives performance.

2 ADDRESS THE HIGHEST RISKS AND VULNERABILITIES FIRST

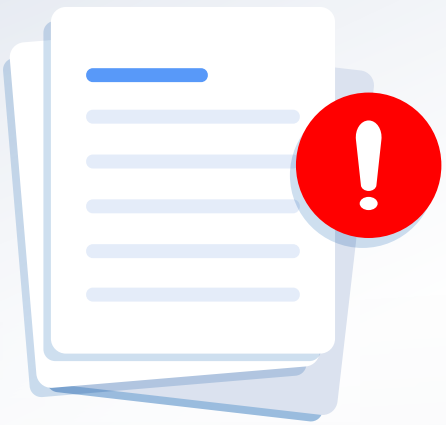
- [ ] To prevent and deal with mishaps, you must have a clear idea of what to prioritize. Since most organizations can't address all problems simultaneously, it's critical to devote the most amount of attention and resources to the crucial issues first.

  Any technology refresh should prioritize addressing the most severe infrastructure vulnerabilities. For example, if your organization is currently dealing with a ransomware attack, updating or upgrading Microsoft 365 is likely to be a lower priority.

- [ ] You can effectively identify high-priority gaps by relying on a solution that provides comprehensive reports following an audit. A solution of this type must be capable of capturing a large number of network assets, users, configurations and vulnerabilities without installing any software, probes or agents. It must also analyze the data to produce professionally formatted, easy-to-understand reports in a matter of minutes.

High-priority vulnerabilities that must be classified as RED can include:

- Failing backups
- Unauthorized users in the network, including former employees and third parties
- Attempted and successful logins by users marked as former employees or third parties
- Unsecured remote connectivity
- Lack of documented operating procedures



3 THEN FOCUS ON WHAT IS IMPORTANT BUT NOT URGENT

- [ ] There will be gaps that must always be on your radar but can wait until the highest priority gaps are addressed. If totally ignored, they can grow into something more severe and cause problems in the future.

  Although these medium-priority gaps may be acceptable in the short term, they should be considered in future technology refresh plans and budgets.

The following vulnerabilities can be classified as medium severity and fall under the YELLOW category:

- Lack of multifactor authentication
- Antivirus software that isn't up to date
- Failure of automated patching system
- Failure to enable account lockout for some computers

4 IF YOUR BUDGET ALLOWS, DEAL WITH WHAT'S RECOMMENDED

- [ ] These gaps are non-critical and can wait to be addressed after high and medium-priority concerns are resolved.

Some of the gaps that fall under the lowest priority or GREEN category are:

- Accounts with passwords that are set to "never expire" but should actually be changed regularly
- On-premises sync issues that have persisted for more than 15 days
- Computers with operating systems that have reached the end of their extended support
- More administrative access than is required

CORTAVO™

Bridging your technology gaps can be difficult, time-consuming and may require IT expertise that your company lacks. Working with a managed service provider like us can relieve you of the hassle while providing you with the peace of mind you need to focus on your business.

Contact us to learn how we can help you prioritize your technology refresh.